



Strong Passwords: Your Essential Guide

If you don't change your password...
SOMEONE ELSE WILL!

Tips and Tricks to a Safe and Secure Password

Passwords work best when they are long and complex.

1. ALWAYS use a dedicated password manager, which is highly secure and will remember all of your strong passwords. If you choose to keep an offline backup, securely write down only your master password in a physical [logbook](#) or safe place.
2. NEVER use personal information such as, phone numbers, names, birthdays, addresses, or repeating or consecutive letters and/or numbers like 1234567890, aaaaaaaa, 123123123, or abacaba, and so on.
3. Passwords should be at least 22 characters long, 30 is preferred, and 40 or more is considered best...length is better than complexity.
4. Passwords should include one or more of the following: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and special characters, (!, @, #, \$, %, ^, &, (,), /, and ~), whatever is allowed.
5. Passwords SHOULD NOT be used for multiple accounts.
6. Passwords can be randomly generated from a website, use number/letter substitutions (like on a license plate), or a phrase from your favorite book, movie, or poem...it's ok to make it easy to remember. If you use a common or well known phrase, mix it up a bit by substituting letters and numbers. Keep in mind, hackers read, watch, and know the current trends.
7. Finally, if your password is immediately compromised. Otherwise update them at least once a year! Using stale passwords can leave you vulnerable to a hack. Be diligent!

For a detailed discussion on passwords and passphrase strategies, visit our blog: [What's In A Password](#)